CHAIN OF TRUST PROCESSING

ABSTRACT

A technique for automatically obtaining a second certificate for a user using a first certificate includes accessing a server platform using a user's server and the first certificate of the user to create a connection that authenticates both the user's server identity via a server certificate of the user server and the user's identity via the user's first certificate. A secure data channel is then created between the server platform and the user platform. A request for the second certificate is forwarded by the user from the user server to the server platform and the server platform then generates the second certificate. The first certificate may be a signature certificate and the second certificate may be an encryption certificate. The first certificate may be an expiring signature certificate and the second certificate may be a replacement signature certificate. The first certificate may be a signature certificate and the second certificate may be a replacement encryption certificate to replace an expiring encryption certificate. The first certificate may be a signature certificate and the second certificate may be one of either the user's current encryption certificate or an expired encryption certificate of the user. Thus, the first certificate may be used as a mechanism for establishing a "chain of trust" that can be used to obtain all

other certificates without requiring the manual intervention of an enterprise officer, thereby considerably reducing the time and expense of obtaining additional certificates for a user.